UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,928	08/09/2001	Rodric C. Fan	TRMB-2096	6041

70409 7590 09/19/2008

TRIMBLE NAVIGATION LIMITED C/O WAGNER BLECHER
123 WESTRIDGE DRIVE
WATSONVILLE, CA 95076

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/927,928	FAN ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6,8-11,15-17,20,25-27 and 29-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6,8-11,15-17,20,25-27 and 29-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to Applicant's Remarks and Amendments filed May 16, 2008.

Claims 5, 7, 12-14, 18-19, 21-24, and 28 remain cancelled.

Claims 1-4, 6, 8-11, 16-17, 20, 26, 27 and 29-33 are amended.

Claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 are pending and herein considered.

Response to Arguments

Applicant's amendments to claims 1-4, 6, 8-11, 16-17, 20, 26, 27 and 29-35 serve to overcome the Examiner's previously set forth claims objections and 35 USC 112 rejections. As such, those objections and rejections have been withdrawn.

Applicant's arguments in response to the Examiner's 35 USC 103(a) rejection of claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 have been fully considered but they are not persuasive. Applicant's sole argument regarding these rejections regards Kaufman and Droge's alleged failure to teach or suggest "utilizing a third key to encrypt the data packet" as taught in claim 1. The Examiner respectfully disagrees, maintaining her position that the Kaufman reference in view of Droge teaches the claims in their entirety. The Droge reference has been relied upon by the Examiner to provide support for the twice encryption of data before transmission. In particular, Droge discloses the encryption of data (payload) a first time such that that data is once encrypted (par

12). Droge then goes on to packetize that data along with a header before encrypting that data a second time so that it may be "twice encrypted" (par 12). Throughout the reference, and in particular throughout paragraphs 50-53, Droge provides additional support for his encryption, including a listing of possible encryption algorithms that may be utilized, including but not limited to DES, Triple DES, AES, SKIPJACK, and BLOWFISH. Droge even goes so far as to provide for the use of two different algorithms (or the same) for the two steps, dependant upon the needs of the user and system. With regards to Applicant's invention in particular, the Examiner has relied upon Droge's DES and Triple DES provisions to teach Applicant's "utilizing a first key to encrypt a payload" and "utilizing a third key to encrypt the data packet." One skilled in the art of cryptography would clearly understand both DES and Triple DES to include the use of a symmetric session key. With regards to the utilization of a second key to encrypt the first key before transmission, although the Examiner has relied upon Kaufman in particular in her actions, she would like to take this opportunity to point out paragraph 66 within Droge which provides for the use of additional "tokens, keys, certificated or other authenticating mechanism[s] to secure transaction[s]" including the use of public/private key pairs to "authenticate a user using digital certificates." This use of public/private key pairs equates to Applicant's encryption of his first key using a second key (public key) so that it may be transmitted to the server/wireline wherein it may be decrypted by the private key associated with that public key. The use of public/private key pairs to authenticate and provide additional security measures is equally well known in

the art and will not be further discussed at this point. Moving on to the Kaufman reference, the Examiner has relied upon its particular teachings regarding the use of a second key, a master key in Kaufman's case, to encrypt a shared/symmetric key before transmission. Although Kaufman calls for the use of "a master key" for each node, these keys equate to Applicant's keys used to encrypt and decrypt his first key. There is no doubt in the mind of the Examiner that the references taken together serve to teach the encryption of a payload using a first key, the encryption of that key by a second key, the packetization of the encrypted first key and the encrypted payload to form a packet which is then encrypted by a third key.

Applicant's arguments concerning claims 6, 10, and 29 rely upon those given above with regards to claim 1. These arguments are equally unpersuasive.

Applicant's arguments concerning the remaining claims are based upon their dependency upon the independent claims discussed above. These arguments are equally unpersuasive.

It is based upon the above made arguments in view of the references in their entirety that the Examiner maintains her 35 USC 103(a) rejection of claims 1-4, 6, 8-11, 16-17, 20, 26, 27 and 29-35, included below in an amended form to reflect Applicant's amendments.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner is unsure how exactly "a first key employs a symmetric key" and what exactly the first session key is employing it for. The Examiner is under the impression that the Applicant meant to claim "wherein the first key is a symmetric key" and will treat the claim as such for purposes of furthering prosecution.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 remain rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 5,081,678 to *Kaufman et al.*, and further in view of United States Patent Application Publication No. 2002/0004898 A1 to *Droge.*

As per **claim 1**, Kaufman teaches a method for transmitting secured data over a wireless link, the method comprising:

utilizing a first key to encrypt a payload (col.3 lines 6-13);

adding a header to the encrypted payload to form a data packet (col.4 lines 59-68);

utilizing a second key to encrypt the first key (col.3 lines 14-20);

transmitting the encrypted first key to a wireline device, wherein the wireline device decrypts the encrypted first key(col.3 lines 14-20); and

transmitting the encrypted data packet over a wireless link to a gateway, decrypting the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network (col.3 lines 21-33);

and utilizing the wireline device and the first key to decrypt the encrypted payload (col.3 lines 51-62)

Kaufman fails to specifically disclose utilizing a third key to encrypt the data packet and decrypting the encrypted data packet at gateway.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second key to provide for heightened security for the information provided in the data packet.

As per **claim 2**, the combined method of Kaufman and Droge wherein the first key comprises a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 3**, the combined method of Kaufman and Droge teaches transmitting the encrypted first key to the wireline device, wherein the wireline device decrypts the encrypted first key using a private key associated with the second key (Droge par.66; Kaufman col.3 lines 27-31).

As per **claim 4**, the combined method of Kaufman and Droge teaches wherein the third key comprises a symmetric session key (Kaufman col.3 lines 6-20).

As per **claim 6**, Kaufman teaches a device for transmitting secured data over a wireless link, the device comprising:

an encryption engine which generates a first key (col.3 lines 6-13), encrypts a payload according to the first key (col.3 lines 6-13), adds a header to

the encrypted payload to form a data packet (col.4 lines 59-68), encrypts the first key according to a second key (col.3 lines 14-20); and

a wireless transceiver coupled to the encryption engine, the wireless transceiver transmitting the encrypted first key to a server (col.3 lines 14-20) and transmitting the encrypted data packet over the wireless link to a gateway which decrypts the encrypted data packet (col.3 lines 21-33) to recreate the encrypted payload and the header (col.3 lines 21-33), and forwards the encrypted payload and the header to the server over an open network (col.3 lines 21-33);

wherein the server decrypts the encrypted first key and decrypts the encrypted payload using the decrypted first key (col.3 lines 27-31).

Kaufman fails to specifically disclose encrypting the data packet according to a second key and decrypting the encrypted data packet at the gateway. Kaufman also fails to specifically disclose a wireless link to the gateway.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also discloses the use of both wireline and wireless networks and links that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already

disclosed second session key to provide for heightened security for the information provided in the data packet as well as the wireless networks and links as described in Droge to provide for increased network flexibility.

As per **claim 8,** the combined method of Kaufman and Droge teaches wherein the payload comprises information regarding a location of the device (Kaufman col.4 lines 59-68).

As per **claim 9**, the combined method of Kaufman and Droge teaches wherein the first key employs a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 10**, Kaufman teaches a method for secured communication between a mobile device and a server on a wide area network, the method comprising:

encrypting a payload at the device using a first session key (col.3 lines 6-13;

encrypting the first session key at the device using a public key(col.3 lines 14-20);

transmitting the encrypted first session key to the server over a link (col.3 lines 14-20);

decrypting the encrypted first session key at the server (col.3 lines 21-33);

adding a header to the encrypted payload to form a data packet at the device (col.4 lines 59-68);

transmitting the data packet from the device to a gateway which recreates the encrypted payload and the header, and forwards the encrypted payload and the header to the server (col.3 lines 21-33);

wherein the server utilizes the decrypted first session key to decrypt the encrypted payload (col.3 lines 27-31).

Kaufman fails to specifically disclose encrypting the data packet according to a second session key and decrypting the encrypted data packet at the gateway. Kaufman also fails to specifically disclose the wireless capabilities provided for within the instant application including the wireless link and mobile device.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also discloses the use of both wireless networks and mobile devices that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second session key to provide for heightened security for the information provided in the data packet as well as the wireless links and devices as described in Droge to provide for increased network flexibility.

As per **claim 11**, the combined method of Kaufman and Droge teaches wherein the decrypting the encrypted first session key at the server further comprises: decrypting the encrypted first session key at the server using a private key associated with the public key (Kaufman col.3 lines 27-31).

As per **claim 15**, the combined method of Kaudman and Droge teaches wherein the payload includes location information (Kaufman col.4 lines 59-68).

As per **claim 16**, the combined method of Kaufman and Droge teaches generating the first session key at the device based on a random number (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 17,** the combined method of Kaufman and Droge teaches wherein the encrypting the payload at the device using the first session key further comprises encrypting the payload at the device using the first session key, wherein the first session key employs an encryption algorithm selected from a group of the encryption algorithms consisting of DESX and DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 20**, the combined method of Kaufman and Droge teaches implementing an encryption algorithm selected from a group of encryption

algorithms consisting of DESX and DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 25**, the combined method of Kaufman and Droge teaches wherein the data packet includes location information (Kaufman col.4 lines 59-68).

As per **claim 26**, the combined method of Kaufman and Droge teaches utilizing a random number ot generate the first key (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 27**, the combined device of Kaufman and Droge teaches a memory coupled to the encryption engine, wherein the memory stores the second key, and wherein the encryption engine accesses the second key from the memory (col.3 lines 6-20).

As per **claim 29**, Kaufman teaches a computer readable medium, comprising program instruction for performing a method comprising:

encrypting a payload according to a first key (col.3 lines 6-13);

adding a header to the encrypted payload to form a data packet (col.4 lines 59-68);

encrypting the first key according to a second key (col.3 lines 14-20);

transmitting the encrypted first key to a server (col.3 lines 14-20); and

transmitting the data packet over the link to a gateway (col.3 lines 21-33), wherein the gateway recreates the encrypted payload and the header (col.3 lines 21-33), and forwards the encrypted payload and the header to the server which decrypts the encrypted first key (Kaufman col.3 lines 27-31) and decrypts the encrypted payload using the decrypted first key (Kaufman col.3 lines 27-31).

Kaufman fails to specifically disclose encrypting the data packet according to a second session key configured for secured communications over a wireless link and decrypting the encrypted data packet. Kaufman also fails to provide for the use of wireless links and devices within his system.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also discloses the use of both wireless networks and mobile devices that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second key to provide for heightened security for the information provided in the data packet as well as the wireless links and devices as described in Droge to provide for increased network flexibility.

As per **claim 30**, the combined method of Kaufman and Droge teaches wherein the first key comprises a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 31**, the combined method of Kaufman and Droge teaches

receiving the data packet at the gateway (Kaufman col.3 lines 27-31);

decrypting the data packet at the gateway according to the third key (Droge paragraph 13);

forwarding the encrypted payload to the server (Droge paragraph 13);

receiving the encrypted first key at the server (Kaufman col.3 lines 27-31);

decrypting the encrypted first key using a fourth key (Kaufman col.3 lines 27-31); and

decrypting the payload according to the decrypted first key (Kaufman col.3 lines 27-31).

As per **claim 32**, the combined method of Kaufman and Droge teaches wherein the first session key comprises a symmetric session key (Kaufman col.3 lines 6-13).

As per claim 33, the combined method of Kaufman and Droge teaches implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 34**, the combined method of Kaufman and Droge teaches wherein the data packet includes location information (Kaufman col.4 lines 59-68).

As per **claim 35**, the combined method of Kaufman and Droge teaches wherein the symmetric session key is generated based on a random number (Kaufman col.5 lines 24-29, col.6 lines 62-68).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137